CLAIMS

1. A cryptographic method of anonymously signing a message by a member of a group comprising n members each equipped with calculation means (25) and associated storage means (24), which method is characterized in that it comprises the following initial steps at the time of constituting the group:

- a first step in which first calculation means of a trusted authority calculate a pair of asymmetric keys (30, 31) common to the members of the group and comprising a common public key (30) and a common private key (31) (operation 1),
- a second step in which the first calculation means calculate a group public key (32) associated with the group (operation 2),
- a third step in which, for each member, during an interaction between the calculation means of the trusted authority and the calculation means of the member, a group private key (33_1) is calculated (operation 3) and stored (operation 4) in the storage means (24) of the member, each group private key (33_1) being associated with the group public key (32) and being different for each member of the group,
- a fourth step in which the first calculation means determine as many symmetrical secret keys (34_i) as there are members of the group (operation 5), and
- a fifth step in which the first calculation means (20) encrypt the common private key (31) using each of the secret keys (34_i) to obtain as many encrypted forms of the common private key (31) as there are non-revoked members (operation 6),

and in that it comprises the following steps on each revocation within the group:

- a sixth step in which the first calculation means (20) modify the pair of common asymmetric keys (31) to determine a common public key (30) and a common private key (31) that are up to date (operation 8),

- a seventh step in which the first calculation means (20) encrypt the common private key (31) using each of the secret keys (34_i) to obtain as many encrypted forms of the common private key (31) as there are non-revoked members (operation 9),

and in that the method comprises the following steps on the group member anonymously signing (operation 10) a message having to be sent to an addressee:

- an eighth step in which the common private key (31) stored by the storage means (24) of the member is updated (operation 11) only if one of the encrypted values of the common private key (31) may be decrypted using the symmetrical secret key (34_1) in the member's storage means (24),
- a ninth step in which the member's calculation means (25) calculate (operation 12) an anonymous signature of the message using its group private key (33_1), and
- a tenth step in which the member's calculation means (24) calculate (operation 13) an additional signature of the combination comprising the message and the anonymous signature using the member's common private key (31).

2. A cryptographic anonymous signature method according to claim 1, wherein the group is constituted at a date t1 and further comprising the following operations:

- during the first step, the first calculation means associate the common private key (31) with an update date equal to t1 (operation 14), and
- during the third step, the storage means (24) of each member store the update date of the common private key (operation 15),

wherein the following operation is executed at the time of each revocation within the group at a date t2:

- during the sixth step, the first calculation means (20) modify the update date to determine an update date equal to the date t2 (operation 16),

and wherein the following operation is executed on each anonymous signing by the member of the group of a message having to be sent to an addressee:

- during the eighth step, the common private key stored in the member's storage means (24) is updated (operation 11) only if the update date (D_1) in the member's storage means (24) is also different from the update date (D) of the common private key (31) updated by the first calculation means.

3. A cryptographic anonymous signature method according to claim 1, further comprising the following operations:

- during the third step, the first calculation means calculate for each member of the group an identifier (35_i) of the member (operation 3) and the identifier (35_i) of each member is stored in the member's storage means (24) (operation 4),

and the following operation on each revocation within the group:

- the first calculation means (20) calculate an identifier (35_i) for each new member of the group.

4. A cryptographic method according to claim 3 of anonymously signing a message, wherein the steps further comprise:

- during the third step, storage means (36) connected to the first calculation means (20) store the symmetrical secret key (34_i) of each member, the group public key (32), the public key (30) common to the members of the group, each of the encrypted forms of the common private key (31), and each of the identifiers (35_i), each encrypted form of the common private key (31) being associated with one of the identifiers (35_i),

and further comprising the following operation for each modification of the composition of the group that corresponds to a revocation of one of the members of the group:

- removing the secret key (34_i) of that member from the storage means (36) connected to the first calculation means (20),

and further comprising the following operations to update the common private key (31) stored in the member's storage means (24):

- the member's calculation means (25) read the different encrypted form (31) of the common private key stored in the storage means (36) connected to the first calculation means (20) and associated with the identifier (35_i) of the member, and
- the member's calculation means (25) decrypt the different encrypted form of the common private key (31) previously read using the secret key (34_i) stored in the member's storage means (24).

5. A cryptographic method according to claim 1 of anonymously signing a message, wherein the initial steps further comprise:

- during the third step, storage means (36) connected to the first calculation means (20) store the secret key of each member, the pair of asymmetric keys (30, 31) common to the members of the group, and the group public key (32),

and further comprising the following operation on each modification of the composition of the group that corresponds to a revocation within the group:

- the secret key of the revoked member is eliminated from the storage means (36) connected to the first calculation means (20),

and further comprising the following operations to update the common private key (31) in a member's storage means (24):

- the member's calculation means (25) read the different encrypted forms of the common private key (31) in the storage means (36) connected to the first calculation means (20), and

- the member's calculation means use the secret key (34_1) in the member's storage means (24) to decrypt the different encrypted forms of the common private key (31).

6. Cryptographic apparatus for anonymously signing a digital message, characterized in that it comprises:

- first calculation means (20) for calculating (operations 1, 2) at least one pair of asymmetric keys (30, 31) common to the members of the group of n members and a group public key (32) associated with the group, for calculating (operation 3) a group private key (33_1) for each member during interaction with the member's calculation means (25), each group private key (33_1) being associated with the group public key (32) and being different for each member of the group, for determining (operation 5) as many symmetrical secret keys (34_i) as there are members of the group and encrypting (operation 6) the common private key (31) using each of the symmetrical secret keys (34_i) to obtain as many encrypted forms of the common private key (31) as there are non-revoked members.

7. Cryptographic apparatus according to claim 6 for anonymously signing a digital message, further comprising:

- storage means (36) connected to the first calculation means (20) via a communications network (23) for storing at least an symmetrical secret key (34_i) of each member of the group, the group public key (32), the public key (30) common to the members of the group, and each of the different encrypted forms of the common private key (31).

8. A smart card (21_1) intended for a member of a group of n members and adapted to interact with apparatus according to either claim 6 or claim 7, characterized in

that it comprises:

- means (24) for storing a private key (31) common to the members of the group, a group private key (33_1) of the member, and a symmetrical secret key (34_1) assigned to the member,
- means (25) for updating the common private key (31) stored in the member's storage means (34) to update (operation 11) the common private key (31) only if one of the encrypted values of the common private key (31) calculated by the first calculation means (20) of the apparatus may be decrypted using the symmetrical secret key (34_1) in the member's storage means (24), and
- calculation means (25) for calculating (operation 12) an anonymous signature for a message using its group private key (33_1) and for calculating (operation 13) an additional signature for the combination comprising the message and the anonymous signature using the member's common private key (31).

9. A smart card (21_1) according to claim 8, wherein the updating means (25) comprises decrypting means for decrypting one of the encrypted values of the common private key (31) calculated (operation 1) by the first calculation means (20) of the apparatus using the symmetrical secret key (34_1) in the member's storage means (24).

10. A cryptographic system for anonymously signing a digital message by implementing a method according to claim 1, characterized in that it comprises at least:

- apparatus according to either claim 6 or claim 7, and
- as many smart cards (21_1) according to claim 8 as there are members in the group.